Testimony of
Dennis M. Lormel
President & CEO
DML Associates, LLC
Lansdowne, Virginia
House Committee on Homeland Security
Subcommittee on Counterterrorism and Intelligence
5/18/2012
"Terrorist Financing Since 9/11: Assessing an Evolving al Qaeda and State Sponsors of Terrorism"

Good morning Chairman Meehan and distinguished members of the Committee. Thank you for inviting me to testify at this hearing. Terrorist financing is a subject that is extremely important to me. This topic does not receive the attention it deserves. I greatly appreciate the fact that you are taking the time to delve into this subject.

There are few events in a lifetime that evoke deep seated emotion and vivid recollection. The terrorist attacks against the United States by al Qaeda on September 11, 2001 (9/11), are clearly one of those historic moments that remain frozen in our minds. I poignantly remember my personal reaction then and how it affects me now. 9/11 changed my life, as it did for so many of us. As the agent in charge of the FBI's Financial Crimes Program at that time, I was in a unique situation where I was afforded an opportunity to respond in a manner few other people could. I was in a position to "follow the money." I witnessed, firsthand, investigative successes which disrupted or deterred funding intended to support terrorist activities. I am an ardent believer that terrorist financing is a critical component of the war against terrorism.

By way of background, immediately after 9/11, I was responsible for the formation and oversight of the FBI led, multi-agency, Financial Review Group, which evolved into a formal Section within the FBI's Counterterrorism Section, known as the Terrorist Financing Operations Section (TFOS). Since retiring from the FBI, I have provided consulting services regarding fraud, money laundering and terrorist financing. Many of my clients are in the financial services sector.

My government investigative and private sector consulting experience has provided me a rare opportunity to understand two very distinct perspectives. For over 30 years, I had a law enforcement perspective. In that capacity, my perspective was government and investigative driven. For the last nine years, in my current position as a consultant, my perspective has shifted to one that is industry and compliance driven. This provides me with a unique understanding of the responsibilities, sensitivities, challenges and frustrations experienced by the government and financial sectors in dealing with anti-money laundering (AML) and terrorist financing considerations. There is a notable difference in perspectives. This is one of the many challenges we face in dealing with terrorist financing and other criminal problems.

Identifying suspicious activity in financial institutions, especially involving terrorist financing, is extremely challenging. This is where understanding perspective is critically important. When it comes

to identifying and reporting suspicious activity, you must consider the "who, what, where, when, why and how." Law enforcement typically focuses on the "why" as the most important element while financial institutions are most concerned about the "how." This is one of the areas where collaboration between law enforcement and financial institutions is not as consistent as it could be. Law enforcement frequently shares "war stories" about investigative successes with industry. However, they do not often provide specific information about "how" financial institutions were used by the bad guys. The Internal Revenue Service is one agency that does provide this type of information to financial institutions at industry training forums.

In order to succeed, individual terrorists, such as lone wolves, and terrorist groups must have access to money. They require funding in order to operate and succeed. Invariably, their funding sources will flow through financial institutions. To function, terrorists must have continuous access to money. Regardless of how nominal or extensive, the funding flow is operationally critical. Terrorists, like criminals, raise, move, store, and spend money in furtherance of their illicit activity. This is why Bank Secrecy Act (BSA) reporting requirements are essential to our National Security. This fact becomes more compelling in view of the actuality that finance is one of the two most significant vulnerabilities to terrorist and criminal organizations.

Terrorist financing is not adequately understood and extremely difficult to identify, especially when funding flows are more nominal. This is where government, through the interagency community engaged in terrorist financing, must interact more efficiently with the financial services sector to identify terrorist financing. It is possible for financial institutions to identify terrorist financing, but it is highly improbable. We must take continual actions that increase the probability factor, thereby increasing the possibility of identifying funding flows. The challenge confronting the government and banking community is to improve the effectiveness of the process. This is where the government needs to be more effective and efficient in the "how" of assisting financial institutions in identifying suspicious activity. Government should develop better feedback mechanisms to financial institutions about "how" terrorists use financial institutions and provide them with typologies that financial institutions could use for transactional monitoring.

The interagency community that has jurisdiction and responsibility for terrorist financing should be commended for their contributions. Terrorist financing is one area where the government excelled following 9/11 and where they continue to perform admirably.

Terrorist financing is every bit as challenging today as it was in the immediate aftermath of 9/11. Law enforcement, regulators and intelligence agencies here, in the United States (U.S.), and abroad, have achieved noteworthy and meaningful accomplishments. New proactive and progressive methodologies have been developed and implemented in furtherance of such efforts. When the government succeeds in implementing and executing proactive methodologies, the ability of terrorists to carry out operations is diminished. However, lingering concerns and the resiliency of terrorists to adapt to change, coupled with the ease of exploitation of systemic vulnerabilities in the financial sector, will perpetuate the challenge of addressing the issues presented by terrorist financing.

Despite the gains we've made, the financial services sector is as inherently vulnerable today as it was on 9/11. On October 3, 2001, as a senior executive in the FBI, I testified before the House Financial Services Committee. One of the issues I addressed was vulnerabilities or high risk areas in the financial services sector. I testified that wire transfers, correspondent banking, fraud and money services businesses were the biggest areas of vulnerability to the financial services industry at that time.

Today, I have refined the vulnerabilities in two categories: crime problems and facilitation tools. The most significant crime problems we currently face in the financial services industry are fraud and money laundering. Fraud was magnified during the recent financial crisis and continues to represent a significant threat to our economy. Money laundering encompasses all other criminal activity where the proceeds of crime are laundered through financial institutions. The key facilitation tools used in furtherance of fraud and money laundering are: wire transfers, correspondent banking, illegal money remitters, shell companies and electronic mechanisms.

Illegal money remitters represent one of the most significant problems confronting banks. This has been an ongoing challenge. Many banks cannot identify customers who operate illegal money remittance operations. On the surface, they appear to be a legitimate business. However, if like the Carnival Ice Cream Shop in Brooklyn, New York, they actually functioned as illegal money remitters funneling money to high risk countries. Consequently, terrorist and criminal groups have used illegal money remitters in furtherance of their illicit activities. There are a number of cases we can point to that illustrate this problem to include the Time Square bombing case.

Sanctions against Iran have caused Iranian entities to regularly use shell companies to hide beneficial ownership, as well as rely on correspondent banking and wire transfers to illegally move funds. The Lloyds Bank "stripping" case is a prime example of how correspondent banking was used by Iran as a facilitation tool. In this matter, Lloyds stripped SWIFT messaging information to hide Iranian bank identification in order to avoid U.S. banking monitoring detection. The Alavi Foundation case was an example of how Iran used shell companies to hide beneficial ownership in a New York City office building. Both cases involved the use of wire transfers.

The use of electronic payment mechanisms is an area of growing concern regarding how terrorists move money due to the anonymity and instant settlement it affords. Electronic payment mechanisms are becoming more prolific and vulnerable to misuse by criminals and terrorists. Africa is a venue of concern for the growing use of electronic mechanisms.

The government has made consistent incremental progress in addressing terrorist financing. Individual agencies and entities responsible for terrorist financing have matured and evolved. They have individually and collectively developed investigative methodologies to effectively deal with the constant and emerging challenges. Although on an agency by agency level, we can point to enhanced capabilities, the true measure of government success is the ability of the interagency community to work as a unified team, and to parlay their collective investigative capabilities into a joint government wide terrorist financing strategy. In the aftermath of 9/11, I was part of such a working group that was led by David Aufhauser, then the General Counsel at the Treasury Department. Mr. Aufhauser was a

true leader who marshaled the interagency collaborative initiative. He was an unsung hero and visionary. I recommend that the Committee periodically assess the status of the interagency terrorist financing working group to ensure that it is effectively coordinating the broader interagency initiatives.

The face of terrorism since 9/11 has been altered significantly. The last few years have seen tremendous change and instability in the Middle East. Core al Qaeda has been decimated and affiliate groups have evolved into greater threats. Our homeland has experienced a growing concern involving lone wolf terrorists and other homegrown threats. These developing factors have modified terrorist financial typologies.

The evolving terrorist landscape has led to less costly terrorist plots. As noted earlier, the more nominal amounts have been more challenging to identify. This is due to the fact they are generally more undetectable. For example, many lone wolf terrorists such as Farooque Ahmed, who plotted to detonate a bomb on the Washington, DC metro system, relied on money from their legitimate jobs to pay for their illicit activity.

The government must continuously identify and assess emerging trends and develop case typologies they can share with financial institutions. In so doing, the financial services sector can implement transaction monitoring strategies to identify patterns of activity consistent with the case typologies of criminals and terrorists. The government has not done this as consistently as they could have.

In general, law enforcement and the Financial Crimes Enforcement Network (FinCEN) have done a good job in sharing information with the financial services sector. However, they have not done as much as they think they have or they could. I do not make this comment lightly. When I was in the FBI, I thought I had maximized liaison relationships. It was not until after my retirement from law enforcement and my consulting work with the financial services sector that I realized I could have done more. It was a matter of perspective. If only I knew then, what I know now, I would have been dangerous. Law enforcement and FinCEN should do a better job of listening and providing feedback to financial institutions in the form of "how" terrorists and criminal organizations use the financial system in furtherance of their illicit activities.

What is important, especially in dealing with more minimal dollar amounts, is identifying case typologies and using them to develop targeted transaction monitoring strategies. This leads to the need for more consistent collaboration between law enforcement and the financial services sector. The model for this type of public and private sector collaboration was set in recent years by JPMorgan Chase under the leadership of compliance executive William Langford and senior investigator Phil DeLuca. Working in conjunction with the ICE Department of Homeland Security Investigations (HSI), JPMorgan Chase was able to identify financial patterns for human smugglers and traffickers. This was because HSI provided specific typologies to JPMorgan Chase setting forth the "how." This enabled JPMorgan Chase to identify patterns of transactional activity and develop targeted transactional monitoring. In so doing, JPMorgan Chase was able to provide HSI with financial intelligence information which led to successful criminal investigations. This initiative was greatly supported by an informal task force involving DHI and the financial services sector that was led by John Byrne and the Association of Anti Money Laundering

Specialists (ACAMS). Because of the successful impact of this public private partnership, ACAMS provided a special award to JPMorgan Chase and HSI, which was presented at the recent Money Laundering.com annual anti-money laundering conference. This is a great example of how law enforcement, in this case HSI, provided the "how" to a financial institution, JPMorgan Chase, and how the bank used the information to identify patterns of illicit activity. I recommend that the Committee look at this collaboration as a model of the type of cooperative initiative that could be used to fight terrorist financing.

This type of initiative could be effectively used to identify terrorist financing. There are a number of scenarios that could be identified and targeted in a similar fashion. An example would be the case of a lone wolf terrorist who leaves the United States and travels to Pakistan to attend a terrorist training camp. During the time that this individual attends the training camp, it is unlikely he or she would incur any financial activity, virtually falling off the financial grid. The combination of travel to Pakistan, a high risk country for terrorism, and a gap in financial activity, could be identified by targeted financial monitoring in a financial institution.

One of the perceived impediments to banks in regard to targeted transactional monitoring is the challenge of satisfying the regulators. Regulators are not generally forward thinkers. They deal with black and white issues and are more prone to a check the box mentality that tends to stymie progressive and innovative thinking. In fairness to regulators, their mandate is not to think outside the box but to ensure that regulatory requirements are met by financial institutions. This is a daunting task. There is often a perplexing triangle involving financial institutions, law enforcement and the regulators. BSA reporting requirements were established to benefit law enforcement. Unfortunately, financial institutions are generally more concerned with placating their regulators than providing the "why" to law enforcement. Financial institutions, law enforcement and regulators need to come to a better consensus about the balance of law enforcement and regulatory considerations. This is an area that this Committee or the House Financial Services Committee should look into.

Certain countries pose a challenge to deal with in terms of their capacity or political will to establish terrorist financing regimes. Other countries, most notably Iran, pose a significant threat and are indifferent to complying with international standards as they flaunt their nuclear and/or other ambitions. The first step to deal with these situations is to coordinate a strong interagency response at the domestic level. This calls for relying on a combination of diplomatic, regulatory, intelligence, military and law enforcement responses. By orchestrating a choreographed response strategy, pressure could be leveraged against these countries. The second step is to coordinate international responses and strategies with the Financial Action Task Force (FATF), the United Nations and other international bodies.

There is a growing and troubling nexus between transnational criminal organizations, drug cartels and terrorist organizations. Each has their own objective and is willing to deal with the others to further their own interests. The Lebanese Canadian Bank investigation manifests this emerging problem. It illustrated the alliance between Hezbollah, a terrorist organization, the Joumaa drug trafficking and money laundering organization in Lebanon, and the Los Zetas Mexican drug cartel. This troubling

alliance relied on drug trafficking and trade based money laundering, among other activities to facilitate the illicit activities of three dangerous transnational groups. The interagency community should closely assess the collaborative operations of these organizations and develop strategies to deal with other similar associations.

As noted earlier, it is possible to identify terrorist financing but highly improbably. This is one area where collaboration and partnership between the public and private sector are essential. In 2009, I wrote an article addressing how to increase the probability through such collaboration. For the most part, the same points I articulated then are applicable today. Accordingly, there are six steps the government and financial services industry should take to collectively and unilaterally increase the probability of identifying terrorist financing. They are:

1. The government and financial sector must recognize the importance of terrorist financing specific training. This is a dimension that is lacking on both sides, although more on the part of financial institutions. Without specific training, the ability to understand and disrupt terrorist financing is more difficult to achieve.

2. The government must develop a means to legally provide security clearances to select personnel in financial institutions in order to share limited intelligence information that could be scrubbed against bank monitoring systems to identify account or transactional information associated with terrorists. The FBI has been discussing this challenging issue since 9/11, in concert with select industry compliance leaders and experts.

3. A consistent and comprehensive feedback mechanism from law enforcement must be developed that demonstrates the importance of BSA reporting, especially the significance of Suspicious Activity Reports (SARs). FinCEN's SAR Activity Review is a good mechanism that provides insightful information. In addition, specific feedback from law enforcement to financial institutions concerning the value and benefit of BSA data, including SAR filings, would have a dramatic impact on the morale of individuals responsible for SAR reporting.

4. There must be an assessment by the government of all SARs related to or identifiable with terrorism cases. Such a review would identify specific red flags that could be used as a training mechanism and more importantly, could be factored into identifying typologies that could be used for the monitoring/surveillance capabilities of financial institutions. In addition, a determination could be made as to why the financial institution filed a SAR. In many instances, the SAR was filed for violations other than terrorist financing. Understanding what triggered the SAR filing; in tandem with how the SAR ultimately was linked to terrorist interests would be insightful.

5. In addition to assessing SARs, the government and industry should collectively identify and assess as many case studies, of terrorist financing related investigations, as can be identified and legally publically accessed. The case studies should be compared to determine what types of

commonalities and patterns of activity exist. In addition, common red flags should be easily discernible. This type of case study assessment, coupled with the SAR analysis, would provide more meaningful information to consider in identifying terrorist financing characteristics, especially in cases involving more nominal financial flows. This would enable financial institutions to more effectively use surveillance and monitor techniques to identify questionable transactional information.

6. A combination of BSA data, particularly SARs, combined with empirical and anecdotal information would enable the government and financial sector to collectively and unilaterally conduct trend analyses. This would be a significant factor in identifying emerging trends. On a government level, this would contribute to implementing investigative and enforcement strategies. On the institutional level, this would enable the financial sector to implement strategies to mitigate risk.

Although the landscape has changed, and methodologies have evolved since 9/11, terrorist financing remains the same. In essence, terrorists must have access to funds when they need them in order to operate. It is incumbent that government agencies cooperate, coordinate and communicate on both an interagency level and with the private sector in order to deny terrorists from moving and accessing funds and thereby diminishing their ability to operate.

I would again like to thank the Committee for affording me the opportunity to participate in this forum. I would be happy to answer any questions or to elaborate on my statement.